

Detector-decoy quantum key distribution without monitoring signal disturbance

Hua-Lei Yin,^{1,2,*} Yao Fu,^{1,2,†} Yingqiu Mao,^{1,2} and Zeng-Bing Chen^{1,2,‡}

¹*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

²*The CAS Center for Excellence in IQIP and the Synergetic Innovation Center for QIQP, University of Science and Technology of China, Hefei, Anhui 230026, China*

The round-robin differential phase-shift quantum key distribution protocol provides a secure way to exchange private information without monitoring conventional disturbances and still maintains a high tolerance of noise, making it desirable for practical implementations of quantum key distribution. However, photon number resolving detectors are required to ensure that the detected signals are single photons in the original protocol. Here, we adopt the detector-decoy method and give the bounds to the fraction of detected events from single photons. Utilizing the advantages of the protocol, we provide a practical method of performing the protocol with desirable performances requiring only threshold single-photon detectors.

PACS numbers: 03.67.Dd, 03.67.Ac, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) allows two legitimate users, typically called Alice and Bob, to share a common bit string with information-theoretic security even in the presence of eavesdroppers [1, 2]. Since the BB84 [1] protocol was proposed, tremendous progress has been made, for example, SARG04 QKD [3], decoy-state QKD [4, 5], measurement-device-independent QKD [6, 7], and device-independent QKD [8], were proposed to enhance the security of quantum communication. The security proof of QKD, which leads to the explicit form of the extractable secure key rate the corresponding protocol provides, is closely related to the original version of Heisenberg's uncertainty principle [9]. It means that any eavesdropper's intervention acquiring the effective private information of quantum states will lead to a disturbance which can be discovered and estimated from a randomly chosen portion of measurement results, namely, monitoring the signal disturbance. The more disturbance that the eavesdropper (Eve) should have caused, the less efficient the QKD protocol will be.

Recently, Sasaki, Yamamoto, and Koashi proposed a ground-breaking approach, a qudit-based protocol, i.e., the round-robin differential phase-shift QKD (RRDPS-QKD) protocol that does not require disturbance monitoring since the limit on leaked information, namely, the portion of the sifted key subjected to privacy amplification, can be acquired in advance and maintains a high tolerance of noise [10]. Since the RRDPS-QKD was proposed, it has been studied both theoretically [11–13] and experimentally [11, 14–16]. According to the original protocol, the phase error estimation can be done after Alice's preparation in advance without considering

Eve's interventions, which makes it independent of the bit error rate and thus incredibly desirable for practical implementations of QKD. Specifically, under ideal circumstances, the RRDPS-QKD protocol can tolerate a high bit error rate, up to almost 50%, which is significantly different from previous QKD protocols [9], such as the qubit-based BB84 protocol, whose bit error rate cannot go beyond 11% based on one way classical post-processing [17]. However, as pointed out by the authors, a realization of this protocol requires Bob to be equipped with photon number resolving detectors (PNR). This is a problem that all experimental implementations of QKD based on qubit encoding today face, the requirement of photon-counting techniques, as their unconditional security is based on single photon transmission, in which Alice sends single photons into insecure quantum channels, and Bob only receives single photons. Yet in practice, this assumption cannot be satisfied due to the fact that weak laser pulses are usually used as the source, which occasionally include more than one photon, and that the eavesdropper may intercept and send multiphotons to the receiver. Therefore, for qubit-based quantum communication protocols [1–6, 18–22], the decoy state method [4, 5] has solved the multiphoton problems at the source with great enhancements, while squash models [23–26] are proposed to solve problems at the detector.

In the RRDPS-QKD protocol [10], a practical vulnerability lies in that Bob's measurement device requires experimentally challenging detectors that are able to discriminate between single photons from two or more photons, i.e., photon number resolving detectors. Laboratories are presently equipped with conventional threshold photon detectors, and while actual PNR detectors are slowly entering commercial use, they are still highly temperature sensitive and can only resolve a limited number of photons received [27]. In fact, all experimental demonstrations of RRDPS-QKD have used threshold single-photon detectors [11, 14–16]. Meanwhile, a recent work suggests that with the use of threshold detectors, security can still be achieved without monitoring the sig-

*Electronic address: hlyin@mail.ustc.edu.cn

†Electronic address: yaofu@mail.ustc.edu.cn

‡Electronic address: zbchen@ustc.edu.cn

nal disturbance by employing a passive delay change at Bob's measurement site [28]. In this paper, we exploit a detector-decoy (DD) method that estimates the photon statistics provided by combining a threshold detector together with a variable attenuator (amplitude modulator) [29] to give the bounds to the fraction of detected events by Bob from single photons. Through simulation and comparison with Ref.[28], we show that with the photon statistics obtained, we have provided a more advantageous method for feasibly realizing the RRDPS-QKD with an enhancement in the key rate results.

II. METHOD

A. RRDPS-QKD protocol

The basic procedures of the RRDPS-QKD protocol are as follows. First, Alice generates a series of pulse trains, each train with a overall random phase. Then, for each train, Alice prepares L weak coherent pulses with the bit information encoded in their phases s_k ,

$$|\psi\rangle = \bigotimes_{k=1}^L |(-1)^{s_k} \alpha\rangle = \bigotimes_{k=1}^L (-1)^{s_k \hat{n}_k} |\alpha\rangle, \quad (1)$$

where $s_k \in \{0, 1\}$, \hat{n}_k is the photon number operator for the k th pulse, α is related to the average photon number per pulse with $|\alpha|^2 = \mu/L$, where μ is the average photon number of each train. From there, Alice sends the quantum states to Bob through an insecure channel. At Bob's measurement site is an unbalanced Mach-Zehnder interferometer (MZI) with a variable delay at the long arm, which is controlled by a random number generator (RNG). He uses the RNG to generate a number $r \in \{1, \dots, L-1\}$, and after some possible intervention from Eve, Bob detects the signal and acquires the indices $\{i, j\}$, where i satisfies $j = i \pm r \pmod{L}$, and announces them via a public channel to Alice. In practice, the outputs of the MZI are adjusted so that superposed pulses of the same phase go to a detector 0, while pulses of opposite phases go to a detector 1. Thus, Alice records her sifted key as $s_A = s_i \oplus s_j$. A schematic diagram of the protocol is shown in Fig.1. Ideally, Bob's measurement outcomes s_B should equal s_A , though in reality it may include some errors. As Bob's random choice is after Eve's disturbance, the information leaked to Eve is very limited because of information causality [30]. Intuitively, Eve seems to have some control over the generation of index i , though it was shown by a virtual measurement scheme proposed in Ref.[10] that her control is in fact rather limited. Therefore, it is possible to ignore the signal disturbance and analyze errors, namely the privacy amplification, based only on the outcomes of Alice and Bob. A crucial condition for the guarantee of this protocol is for Bob to only declare a detection event successful when one photon is exactly detected by his detector and no other detection occurs along the rest of the pulse.

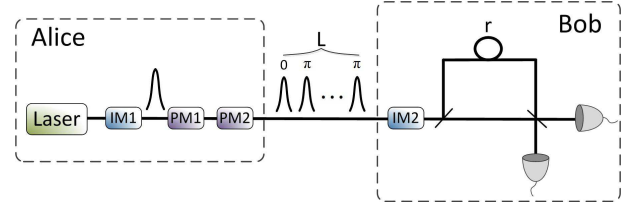


FIG. 1: (Color online) Basic setup of a detector-decoy RRDPS-QKD. IM, intensity modulator; PM, phase modulator; r , the variable delay that generates random numbers from 0 to $L-1$. Here, IM2 realizes Bob's detector-decoy method, PM1 adds a random phase on each pulse train, and PM2 encodes random phases 0 or π on each pulse.

In the following, we show how the single photon detection condition is satisfied with our simple detector-decoy method under current technology.

B. Detector-decoy method

The detector-decoy method, termed by Moroder *et al* [29] to emphasize its connection and applicability in QKD, is outlined thus. Suppose an initial phase randomized signal state (written as a classical mixture of Fock states) of $\rho_{\text{in}} = \sum_{n=0}^{\infty} p_n |n\rangle\langle n|$ [31], with $\sum_{n=0}^{\infty} p_n = 1$ and n being the photon number, passes through intensity modulator (IM) with a transmittance η , and is detected by a threshold detector. The detection operation can be characterized by two operators, receiving no photons that results in no clicks $F_{\text{vac}}(\eta)$, and receiving at least one photon giving exactly one click $F_{\text{click}}(\eta)$, where $F_{\text{vac}}(\eta) = \sum_{n=0}^{\infty} (1-\eta)^n |n\rangle\langle n|$ and $F_{\text{click}}(\eta) = \mathbb{1} - F_{\text{vac}}(\eta)$, $\mathbb{1}$ is the unit operator. Therefore, the probability of receiving no clicks is $p_{\text{vac}}(\eta) = \text{Tr}[F_{\text{vac}}(\eta)\rho_{\text{in}}] = \sum_{n=0}^{\infty} (1-\eta)^n p_n$. Notice that if we were to variate the transmittance $\eta = \{\eta_1, \eta_2, \eta_3, \dots, \eta_M\}$, in principle, we would be able to obtain a sufficient set of linear functions to solve the unknown parameters, the photon probabilities p_n , thereby attaining the received photon number statistics,

$$\begin{aligned} p_{\text{vac}}(\eta_1) &= \sum_{n=0}^{\infty} (1-\eta_1)^n p_n \\ &\vdots \\ p_{\text{vac}}(\eta_M) &= \sum_{n=0}^{\infty} (1-\eta_M)^n p_n. \end{aligned} \quad (2)$$

In an actual setting, for the detector's imperfections, such as finite detection efficiency η_d and a dark count probability ϵ , we modify the operator $F_{\text{vac}}(\eta)$ as $F_{\text{vac}}(\eta) = (1-\epsilon) \sum_{n=0}^{\infty} (1-\eta\eta_d)^n |n\rangle\langle n|$, and $p_{\text{vac}}(\eta)$ will take the form of $p_{\text{vac}}(\eta) = (1-\epsilon) \sum_{n=0}^{\infty} (1-\eta\eta_d)^n p_n$. Following the ideal detector case, we can also vary the transmittance of the IM to obtain a set of linear func-

tions to deduce the values of p_n and thus gain the signal photon number statistics.

C. Key rate

With the detector-decoy method, we obtain the signal photon number statistics required for the RRDPs protocol key rate generation. In our simulation model, we vary the transmittance of Bob's detector three times, $\eta = \{\eta_1, \eta_2, \eta_3\}$, specifically $\eta_1 = 1, \eta_2 = 0.8, \eta_3 = 0.6$, so that the probabilities of receiving clicks can be written as

$$\begin{aligned} T_1 &= 1 - (1 - p_d) \sum_{i=0}^{10} (1 - \eta_1 \eta_d)^i p_i, \\ T_2 &= 1 - (1 - p_d) \sum_{i=0}^{10} (1 - \eta_2 \eta_d)^i p_i, \\ T_3 &= 1 - (1 - p_d) \sum_{i=0}^{10} (1 - \eta_3 \eta_d)^i p_i, \end{aligned} \quad (3)$$

with p_d as the total dark count probability of each train and η_d as the detector efficiency. Here, we assume that events in which the signals received by Bob that involve more than 10 photons are highly improbable and thus ignored. Next, we calculate a related value, the rate of detection Q_k can be directly measured experimentally. Following methods of the decoy state QKD [4, 5], we have

$$\begin{aligned} Y_i^k &= 1 - (1 - p_d)(1 - \eta_t \eta_k \eta_d)^i, \\ Q_k &= \sum_{i=0}^{\infty} e^{-\mu} \frac{\mu^i}{i!} Y_i^k \\ &= 1 - (1 - p_d)e^{-\mu \eta_t \eta_k \eta_d}, \end{aligned} \quad (4)$$

where $k = 1, 2, 3$ and $\eta_t = 10^{-\beta d/10}$ is the efficiency of transmission related to the transmission distance d and β is the channel loss rate of the fiber. Clearly, with each attenuation of η_k , Q_k should equal the corresponding probability T_k of receiving a click in the detector, and therefore this will be used as constraints in subsequent calculations. In the RRDPs protocol, Bob only declares a detection event successful when single photons are registered by his PNR detector, and the multiphoton signals received are discarded. Here, we consider a more realistic scenario, in which despite signals of multiphotons created by the source or the eavesdropper, throughout transmission and detection, only one photon from each multiphoton signal pulse survives for registration at the detector, while all other photons are lost, mathematically put as a minimum of a single photon transmission probability function,

$$G = \sum_{n=0}^{10} n \eta_d (1 - \eta_d)^{n-1} p_n, \quad (5)$$

under the constraints that $Q_k = T_k$ for $k = 1, 2, 3$, where the photon number probabilities p_n satisfy $\sum_{n=0}^{10} p_n = 1$ and $0 \leq p_n \leq 1$. Meanwhile, in general QKD protocols, the length of secure key K_1 is obtained after subtracting the bits used for error reconciliation and privacy amplification [10], written as $K_1 = N[1 - fH_{\text{ER}} - H_{\text{PA}}]$, where N is the length of the sifted key, H_{ER} and H_{PA} are the costs for error reconciliation and privacy amplification, respectively, and f is the parameter related to the efficiency of the employed error correction code. In standard calculations, it holds that $H_{\text{ER}} = h(e_b)$ and $H_{\text{PA}} = h(e_{\text{ph}})$, where $h(x)$ is the Shannon entropy $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$, e_b and e_{ph} are the bit error rate and phase error rate. In our computations, we inspect specifically the key rate per pulse, with its formula written as [10]

$$\begin{aligned} K_2 &= \frac{1}{L} \left(G_{\min} - Q f h(e_b) - [e_{\text{src}} \right. \\ &\quad \left. + (G_{\min} - e_{\text{src}}) h\left(\frac{v_{\text{th}}}{L-1}\right)] \right), \end{aligned} \quad (6)$$

where Q is the overall gain, G_{\min} is the lower bound of Eq.(5), and e_{src} is a constant associated with the probability of finding more than v_{th} photons in each pulse, written as [10]

$$P(n > v_{\text{th}}) \leq e_{\text{src}} = 1 - \sum_{i=0}^{v_{\text{th}}} e^{-\mu} \frac{\mu^i}{i!}. \quad (7)$$

As we can see, the second and third terms in Eq.(6) are the error correction and privacy amplification terms, respectively.

III. SIMULATION RESULTS

In our simulation, the exact forms of Q and e_b in Eq.(6) can be given by [32]

$$\begin{aligned} Q &= 1 - (1 - p_d)e^{-\mu \eta_t \eta_d}, \\ e_b &= [e_d(1 - p_d)(1 - e^{-\mu \eta_t \eta_d}) + \frac{1}{2}p_d]/Q, \end{aligned} \quad (8)$$

where e_d as the system error probability, and the RRDPs-QKD experimental parameters [14] used are listed in Table I.

TABLE I: Key parameters for simulation.

p_d	η_d	e_d	f	$\beta(\text{dB/km})$
$1 \times 10^{-9}L$	19%	1.5%	1.16	0.2

Considering the worst case of the lower bound of G , where only one photon from each pulse of multiphoton signals survives transmission for registration at the detector, we optimize parameters μ , the average photon number of each train, and v_{th} , the threshold photon number

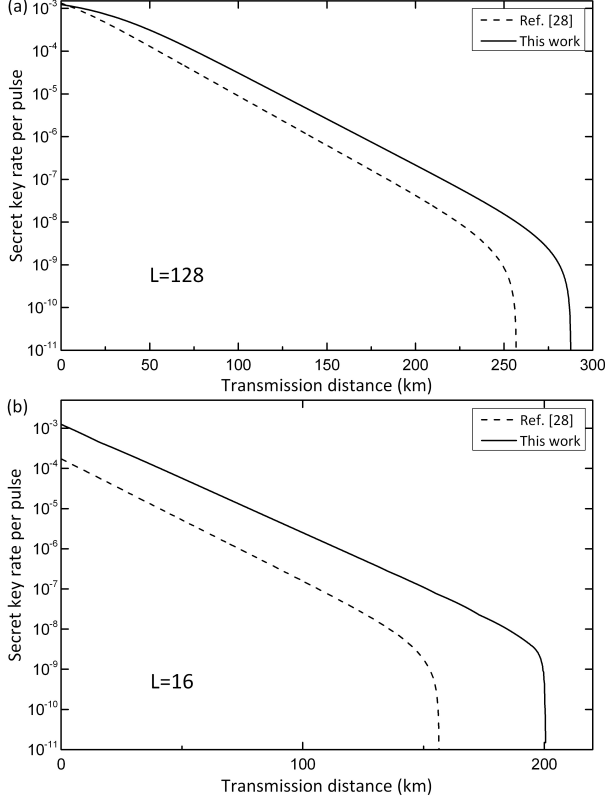


FIG. 2: The optimized secret key rate per pulse for (a) $L = 128$ and (b) $L = 16$ in logarithmic scale as a function of the transmission distance. Our results (solid lines) show that after full optimization of the signal state μ and threshold photon number v_{th} for each value of distance, the detector-decoy-based RRDPS-QKD gives higher optimal key rates and longer performance distances than the methods proposed in [28], depicted as the dashed lines. In order to obtain nonzero key rates with our method at the transmission distance limit of 290 km for $L = 128$, μ and v_{th} were optimized to 4.895 and 20 respectively, and 0.0535 and 3 respectively for $L = 16$ at the transmission distance limit of 200 km.

via a local search algorithm [33] to obtain the optimal key rate per pulse K_2 as a function of transmission distance. The results are shown as the solid lines in Fig.2, for $L = 128$ and 16, from which we can see, our DD-RRDPS-QKD is an experimentally realizable protocol with desirable performance. We also give the full parameter optimized results of the recent implementation of RRDPS also using threshold detectors with a passive delay change [28] with the same simulation experimental parameters as our model (shown as the dashed lines in Fig.2) for comparison, where the key rate per pulse function K_3 is given as Eq.(2) of Ref.[28]

$$K_3 = \frac{1}{L} \left(Q - Qf h(e_b) - [e_{src} + (Q - e_{src})h(\frac{2v_{th}}{L})] \right). \quad (9)$$

As one can see, our results offer significant improvement

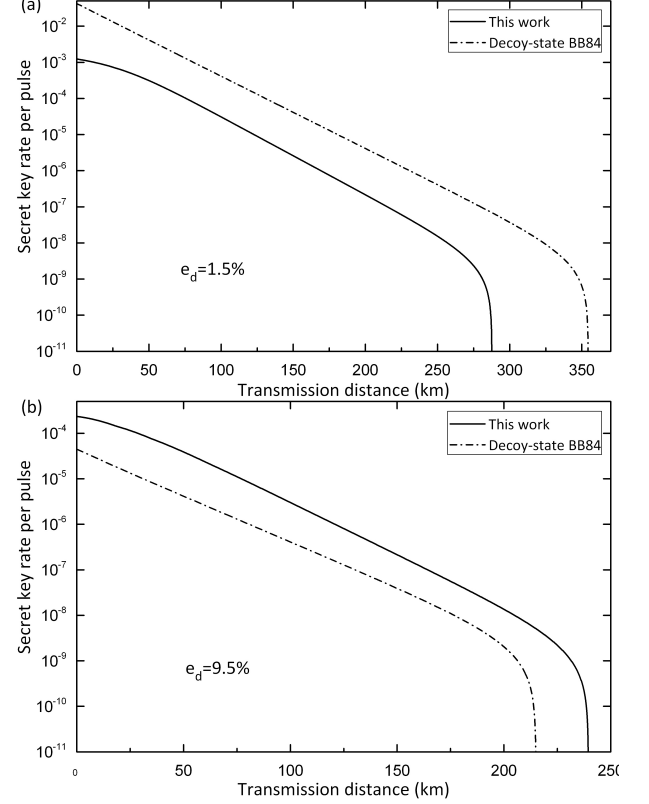


FIG. 3: The optimized secret key rate per pulse for DD-RRDPS (solid lines) and BB84 with infinite decoy states [32] (dash-dotted lines) in logarithmic scale as a function of the transmission distance when $L = 128$. (a) The key rates for $e_d = 1.5\%$. (b) The key rates for $e_d = 9.5\%$.

in both key rate and transmission distance for a given pulse number L compared with the methods proposed in [28]. Moreover, when L becomes fewer, the advantages of our method become more prominent, as it offers more than one order of magnitude higher key rate per pulse at shorter distances to over two orders of magnitude higher key rate per pulse for longer distances, and greater performance distance of almost more than 50 km compared to [28].

Furthermore, we give a comparison between our DD-RRDPS with conventional decoy-state BB84 [32], shown in Fig.3. As one can see, when e_d is small, the decoy-state BB84 outperforms the RRDPS, while as e_d becomes larger, the advantages of RRDPS becomes more prominent. This can be explained by that while e_d is small, p_d plays a significant role in QBER, and since RRDPS encodes only one bit on L pulses, the total detector dark count probability magnifies greatly and the average photon number per pulse decreases significantly, therefore limiting its transmission distance and secret key rate, whereas BB84 encodes one bit per pulse. However, when e_d becomes very large, it will cost a very large portion of the key for privacy amplification in the BB84-QKD protocol, while for RRDPS-QKD, because of its high tol-

erance of errors, privacy amplification has nothing to do with the bit error rate. Therefore, the RRDPS greatly surpasses decoy-state BB84 given that the bit error rate is very large.

IV. CONCLUSION

In conclusion, we have proposed a DD-RRDPS-QKD protocol that by using a threshold detector and a variable attenuator, a practical experimental implementation of RRDPS with desirable key rate and transmission distance has been achieved. With our simulation results, we have given the bounds to the fraction of detected events by Bob from single photons and proved our work to be

an experimentally realizable RRDPS protocol with better performance, even in the worst scenario of only one photon from the entire weak signal of multiphoton pulses is detected by the detector, and have shown that the results obtained in our protocol greatly surpasses recent works. Thus, an immediately feasible experimental solution of the RRDPS-QKD protocol under current technology is offered requiring only threshold single-photon detectors.

Acknowledgments

This work has been supported by the Chinese Academy of Sciences, the National Natural Science Foundation of China under Grant No. 61125502.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984) pp. 175–179.
 - [2] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [3] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, *Phys. Rev. Lett.* **92**, 057901 (2004).
 - [4] H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).
 - [5] X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).
 - [6] H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).
 - [7] S. L. Braunstein and S. Pirandola, *Phys. Rev. Lett.* **108**, 130502 (2012).
 - [8] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007).
 - [9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
 - [10] T. Sasaki, Y. Yamamoto, and M. Koashi, *Nature* **509**, 475 (2014).
 - [11] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, *Phys. Rev. Lett.* **114**, 180502 (2015).
 - [12] Z. Zhang, X. Yuan, Z. Cao, and X. Ma, arXiv:1505.02481 (2015).
 - [13] A. Mizutani, N. Imoto, and K. Tamaki, *Phys. Rev. A* **92**, 060303 (2015).
 - [14] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, *Nat. Photon.* **9**, 827 (2015).
 - [15] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, *Nature Photon.* **9**, 832 (2015).
 - [16] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan, arXiv:1505.08142 (2015).
 - [17] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
 - [18] H.-L. Yin, W.-F. Cao, Y. Fu, Y.-L. Tang, Y. Liu, T.-Y. Chen, and Z.-B. Chen, *Opt. Lett.* **39**, 5451 (2014).
 - [19] X. Ma and M. Razavi, *Phys. Rev. A* **86**, 062319 (2012).
 - [20] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, *Phys. Rev. Lett.* **114**, 090501 (2015).
 - [21] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, *Phys. Rev. A* **91**, 032318 (2015).
 - [22] H.-L. Yin, Y. Fu, and Z.-B. Chen, arXiv:1507.03333 (2015).
 - [23] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Quantum Inf. Comput.* **4**, 325 (2004).
 - [24] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, *Phys. Rev. Lett.* **101**, 093601 (2008).
 - [25] C.-H. F. Fung, H. F. Chau, and H.-K. Lo, *Phys. Rev. A* **84**, 020303 (2011).
 - [26] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, *Phys. Rev. A* **89**, 012325 (2014).
 - [27] O. Thomas, Z. Yuan, and A. Shields, *Nature Commun.* **3**, 644 (2012).
 - [28] T. Sasaki and M. Koashi, “Round-robin differential phase-shift quantum key distribution protocol with threshold detectors,” http://2015.qcrypt.net/wp-content/uploads/2015/09/Poster29_Toshihiko-Sasaki.pdf (2015).
 - [29] T. Moroder, M. Curty, and N. Lütkenhaus, *New J. Phys.* **11**, 045008 (2009).
 - [30] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, *Nature* **461**, 1101 (2009).
 - [31] Y. Zhao, B. Qi, and H.-K. Lo, *Phys. Rev. A* **77**, 052327 (2008).
 - [32] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, *Phys. Rev. A* **72**, 012326 (2005).
 - [33] F. Xu, H. Xu, and H.-K. Lo, *Phys. Rev. A* **89**, 052333 (2014).